UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,385	06/19/2002	Tobias Martin	520.1007	3809

23280 7590 08/10/2006

DAVIDSON, DAVIDSON & KAPPEL, LLC
485 SEVENTH AVENUE, 14TH FLOOR
NEW YORK, NY 10018

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 08/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/049,385	MARTIN ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3-6* is/are pending in the application.

4a) Of the above claim(s) *3 and 4* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *5 and 6* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20020211, 20050202*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Applicant's election without traverse of Group II, Claims 5 and 6, in the reply filed on 22 May 2006 is acknowledged.

2. Claims 3 and 4 withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected invention, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 22 May 2006.

Specification

3. The disclosure is objected to because of the following informalities:

The specification appears to contain minor typographical and other errors. For example, in paragraph 0002, in line 3 of the paragraph, it appears that "being able" is intended to read "are able". In paragraph 0018, line 2, it appears that "$k^{ij} = k^{ij}$" is intended to read "$k^{ij} = k^{ji}$". In paragraph 0024, in step 2, it appears that "Subscribes B and C" is intended to read "Subscribers B and C". In paragraph 0026 (as amended by the preliminary amendment), it appears that the references to steps b, c, and d of the method are intended to refer to steps 2, 3, and 4 as described in paragraph 0042. Further in paragraph 0026, in line 5, it appears that "it being required for (x1, x2, ..., xn)" is intended to read "it being required for h(x1, x2, ..., xn)".

Appropriate correction is required. Applicant's cooperation is requested in correcting any other errors of which applicant may become aware in the specification.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 5 and 6 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Specifically, Claims 5 and 6 are directed to methods for establishing a key. The result of those methods is the determination of a common key, which produces neither a physical transformation nor a concrete, tangible, and useful result. Although the determination of an encryption key is likely to be both concrete and useful, it is not a tangible result. Similarly, determination of such a key does not cause any physical transformation. Therefore, the methods are directed only to an abstract idea, which is non-statutory subject matter. See MPEP § 2106 IV.B.2(b).

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 5 and 6 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 5 recites the limitation "determining a common key k by each subscriber Ti using the values Ni and Nj, $j \neq i$, and the random number z1 sent by the first subscriber T1 in encrypted form using $k := h(z1, g^{z2}, \ldots, g^{zn})$". First, regarding the recited variable "zn", the Examiner notes that although the general random number zi has been defined for each subscriber Ti, the variable "n" is nowhere defined in the claims. Further, the Examiner notes the correspondence between the values Ni, Nj, and the $g^{z2} \ldots g^{zn}$. However, it is not clear from the claims how each subscriber Ti ($i \neq 1$) has access to the values Nj, where $j \neq i$, as it appears that each subscriber Ti only has access to its own value Ni, but not those of the other subscribers Tj. Further, it is not clear how the subscribers Ti ($i \neq 1$) have access to the random number z1. Although z1 is sent to each subscriber from the first subscriber T1, it is sent encrypted with transmission key k^{1j}. It is not clear how each subscriber Tj ($j \neq 1$) has access to the transmission key k^{1j} since the key depends on both Nj, which subscriber Tj possesses (having generated that value in the first claimed step), and z1, which subscriber Tj does not appear to possess, having received only the encrypted form of z1. That is, it appears that to decrypt the value z1, the subscribers Tj ($j \neq 1$) must already have access to z1 in order to generate the key for decryption. The above inconsistencies render the claims indefinite, as it appears that steps are missing which would provide for the receipt by each subscriber Ti of the values Nj ($j \neq i$) and also for the receipt or calculation of the

symmetric decryption key that would allow decryption of the encrypted random number z1. The Examiner notes that it is not clear from the specification exactly how the omission of such steps would be remedied, and therefore it is not possible to fully determine the scope of the claims for interpretation of the prior art, as noted below.

Claim 6 recites the variable "k^{j1}"; however, the variable is not defined or used anywhere in either Claim 5 or Claim 6. Claim 6 further recites the limitation "the key"; however, it is not clear if this refers to the common key or one of the transmission keys.

Examiner's Note

8. Because the claims are rendered indefinite by the several issues detailed above in reference to the rejection under 35 U.S.C. 112, second paragraph, it has not been possible to determine the scope of the claims, and therefore it has not been possible to fully search the prior art for the claimed subject matter in order to make a determination regarding the patentability of the claims with respect to novelty under 35 U.S.C. 102 and non-obviousness under 35 U.S.C. 103. A search has been made to the extent possible, and documents which appear to be relevant are cited below.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Schneier, *Applied Cryptography*, generally discloses conference keying schemes.

b. Fiat, US Patent 5592552, discloses an encryption system including agreement of a group on a common key for the group, where the key can be generated with or without input from all of the members of the group.

c. Peyravian et al, US Patent 6363154, discloses establishment of a group key where the key is based on generation of random numbers at a node of the group.

d. Ingemarsson et al, "A Conference Key Distribution System", discloses a system for establishing a key in a group derived from Diffie Hellman key distribution.

e. Laih et al, "On the Design of Conference Key Distribution Systems for the Broadcasting Networks", analyzes the several group key establishment protocols and discloses a system for establishing a group key based on a threshold scheme.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER